Amendments in the Claims

1. (Previously Presented) A network security system, comprising:

a static policy data store having a static policy data attribute;

a dynamic policy data store for tracking a threat level associated with a connection~~, the dynamic policy data store having a dynamic policy data attribute~~; and

an authorization enforcement facility (AEF) in communication with the static policy data store and the dynamic policy data store and operable to:

perform a risk-aware analysis of the connection to determine the threat level associated with the connection based at least in part on the static policy data attribute, and

store the determined threat level in the dynamic policy data store as a dynamic policy data attribute.

2. (Previously Presented) The network security system of claim 1, wherein the static policy data store comprises at least one of a constraint, a role, a node-role assignment, a threshold value, a node value, a service value, or an action value.

3. (Previously Presented) The network security system of claim 2, wherein the threshold value is inversely proportional to the node value.

4. (Previously Presented) The network security system of claim 2, wherein the threshold value is inversely proportional to the service value.

5. (Previously Presented) The network security system of claim 1, wherein the dynamic policy data store comprises a threat level table.

6. (Previously Presented) The network security system of claim 1, wherein the AEF is further operable to generate a response to the connection.

7. (Previously Presented) The network security system of claim 6, wherein the response comprises at least one of blocking the source of the connection from connecting to an intended destination, altering the intended destination of the connection, or auditing the connection.

8. (Previously Presented) The network security system of claim 1, wherein the AEF is further operable to generate a countermeasure.

9. (Previously Presented) The network security system of claim 8, wherein the countermeasure comprises an active countermeasure or a passive countermeasure.

10. (Previously Presented) The network security system of claim 1, wherein the AEF comprises a router, a gateway, a hardware appliance, or a web server.

11. (Previously Presented) The network security system of claim 1, further comprising a firewall in communication with the AEF.

12. (Previously Presented) The network security system of claim 1, further comprising an intrusion detection system in communication with the AEF.

13. (Previously Presented) A method comprising:

receiving a static policy data attribute from a static policy data store;

receiving a connection request directed to a node;

determining a threat level associated with the connection request based at least in part on the static policy data attribute; and

storing the threat level associated with the connection request as a dynamic policy data attribute in a dynamic policy data store.

14. (Previously Presented) The method of claim 13, further comprising responding to the connection request.

15. (Previously Presented) The method of claim 14, wherein responding comprises at least one of forwarding the connection request to the node; blocking the source of the connection from connecting to an intended destination, altering the intended destination of the connection, or auditing the connection.

16. (Previously Presented) The method of claim 13, further comprising updating the dynamic policy data attribute in the dynamic policy data store based on a result of the determination.

17. (Previously Presented) The method of claim 16, wherein the updating comprises increasing the threat level if the connection request is determined to be anomalous.

20. (New) A network security system, comprising:

a static policy data store having a static policy data attribute comprising at least one of a constraint, a role, a node-role assignment, a threshold value, a node value, a service value, or an action value;

a dynamic policy data store for tracking a threat level associated with a connection; and

an authorization enforcement facility (AEF) in communication with the static policy data store and the dynamic policy data store and operable to:

perform a risk-aware analysis of the connection to determine the threat level associated with the connection based at least in part on the static policy data attribute,

store the determined threat level in the dynamic policy data store as a dynamic policy data attribute in a threat level table, and

generate a countermeasure, the countermeasure comprising an active countermeasure or a passive countermeasure.

.